In the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) A method for detecting and cleaning computer viruses, comprising the steps of:

simulating in a computer a virtual computer circumstance, [[~~on which virtual computer circumstance the~~]] wherein computer viruses will reside on the virtual computer circumstance;

providing a plurality of objects to be infected by computer viruses that induce virus infection;

loading a target object to be scanned into said simulated virtual computer circumstance, said target object being a host possibly attached by a virus;

activating any virus attached on the target object to be scanned in said simulated virtual computer circumstance to induce virus infection of the [[~~target object~~]] plurality of objects and generating standard samples which have been infected, wherein if a virus is attached to the target object and the virus is activated, the target object will include a host body and a virus body;

comparing the plurality of objects after processing in the activating step with the plurality of objects to be infected originally provided[[,]] and determining whether there is any change or not, if there is a change, the target object to be scanned contains a virus, otherwise the target object to be scanned is free of viruses;

analyzing the generated standard samples and extracting information on the viruses indicated by changes between the plurality of objects before infection and the standard samples after infection when it is determined that said target object to be scanned contains a virus, said information including at least the size of the virus and key information of the host which has been changed by the virus; and

cleaning the virus from the infected target object by locating the host body and the virus body in the target object after the activation step, restoring [[~~unchanged~~]] modified key information of the host on the basis of said information, and removing the virus body from the target object after the activation step according to the virus size.

2. (Cancelled)

3. (Previously presented) The method according to claim 1, wherein said computer simulation step includes providing functional functions to call and execute the steps of:

simulating a Central Processing Unit (CPU) by simulating instructions of the CPU;

simulating an Operating System (OS) by simulating various services and various data structures provided by the OS;

simulating peripheral storage devices by simulating storage space and structures of various peripheral storage devices including simulated hard disk and floppy disk and the like; and

simulating a memory by generating, distributing and managing a simulated memory space.

4. (Previously presented) The method according to claim 3, wherein said provided objects to be infected includes baits that have different sizes and contents for inducing viruses of different types and infection conditions.

5. (Currently amended) The method according to claim 4, wherein a plurality of baits having different sizes and contents are provided for a given virus type to satisfy[[-]] the infection conditions of the viruses attached in the target object to be scanned.

6. (Original) The method according to claim 5, further comprising the step of simulating the system time to generate virtual system date and time for inducing the viruses that are sensitive to date and time.

7-8. (Cancelled)

9. (Previously presented) The method according to claim 3, wherein in the step of simulating the peripheral storage device, a memory space is assigned in the memory to simulate a virtual hard disk including three-dimension space by sector number, track number and cylinder

number, a primary boot sector and corresponding blank sector of the No. 0 track , and next boot sector, File Allocation Table, root directory sector, system files, and bait files for inducing viruses.

10. (Previously presented) The method according to claim 3, wherein in the step of simulating the peripheral storage device, a memory space is assigned in the memory to simulate a virtual floppy disk including a boot sector, a File Allocation Table, a root directory sector, system files, and bait files for inducing viruses.

11. (Currently amended) A computer system including a general computer for detecting and cleaning computer viruses, comprising:

a computer simulation unit for simulating in a virtual computer circumstance, [[environment, on which virtual computer environment the]] wherein computer viruses will reside on the virtual computer circumstance;

a plurality of objects to be infected by computer viruses that induce virus infection;

a control unit for loading a target object to be scanned into said simulated virtual computer circumstance, said target object being a host possibly infected by a virus;

a virus infection inducing unit for activating any virus [[possibly]] attached on the target object to be scanned in said simulated virtual computer [[environment]] circumstance to induce virus infection of [[said target object]] the plurality of objects and generating standard samples which have been infected, wherein if a virus is attached to the target object and the virus is activated, the target object will include a host body and a virus body;

a virus decision unit for comparing the plurality of objects after processing in the virus infection inducing unit with the plurality of objects to be infected originally provided[[,]] and determining whether there is any change or not; if there is a change, the target object to be scanned contains a virus, otherwise the target object to be scanned is free of viruses;

a virus analyzing means for analyzing the generated standard samples and extracting information on the viruses indicated by changes between the plurality of objects before infection and the standard samples after infection when it is determined that said target object to be

scanned contains a virus, said information including at least size of the virus and key information of the host which has been changed by the virus; and

a virus cleaning unit for cleaning the virus from the infected target object by locating the host body and virus body in the target object after activation, restoring [[~~unchanged~~]] modified key information of the host according to said information and removing the virus body from the target object after activation according to the virus size.

12. (Canceled)

13. (Previously presented) The system according to claim 11, wherein said computer simulation unit includes:

a Central Processing Unit (CPU) simulation unit for simulating instructions of the CPU;

an Operating System (OS) simulation unit for simulating various services and various data structures provided by the OS;

a peripheral storage device simulation unit for simulating storage space and structures of various peripheral storage devices including simulated hard disk, floppy disk and the like; and

a memory simulation unit for generating, distributing and managing a simulated memory space,

wherein said respective units include functional functions available to be called and allocated memory space, and are independent from specific CPU, OS, and peripheral storage devices.

14. (Previously presented) The system according to claim 13, wherein said provided objects to be infected include baits that have different sizes and contents for inducing viruses of different types and infection conditions.

15. (Previously presented) The system according to claim 14, wherein a plurality of baits having different sizes and contents are provided for a given virus type to satisfy the infection conditions of the viruses attached in the target object to be scanned.

16. (Original) The system according to claim 15, further comprises a system time simulation unit for generating virtual system date and time to induce the viruses that are sensitive to date and time.

17-18. (Cancelled)

19. (Previously presented) The system according to claim 13, wherein said peripheral storage devices simulation unit assigns a memory space in the memory to simulate a virtual hard disk including three-dimension space by sector number, track number and cylinder number, a primary boot sector and corresponding blank sector of the No. 0 track, and next boot sector, File Allocation Table, root directory sector, system files, and bait files for inducing viruses.

20. (Previously presented) The system according to claim 13, wherein said peripheral storage devices simulation unit assigns a memory space in the memory to simulate a virtual floppy disk including a boot sector, a File Allocation Table, a root directory sector, system files, and bait files for inducing viruses.

21 (Previously presented) A computer readable recording medium for causing a computer to execute the steps of the method described in claim 1.

22 (Cancelled)